



FCS TECH TALK

Your Trusted
Technology Partner Since 1989

INSIDE THIS ISSUE:

- How Managed IT Saves Your Business Money
- Monthly Product Spotlight
- Summer Heat..Shorter Laptop Lifespan?



- How to Safely Open a Docusign
- Why Rebooting Your Computer is Important
- Microsoft Windows 11 Update

HOW MANAGED IT SAVES YOUR BUSINESS MONEY—EVEN WHEN NOTHING BREAKS

When many business owners think about IT support, they picture calling someone only when a computer crashes, the internet goes down, or an employee can't access their email.

While fixing problems is certainly part of IT, it's only a small piece of what modern managed IT services provide.

The real value comes from preventing problems before they happen.

Just like routine maintenance keeps a vehicle running reliably and helps avoid expensive repairs, proactive IT management keeps your technology healthy, secure, and operating efficiently. Many of the biggest savings come from issues that never occur because they were prevented in the first place.

Businesses that invest in preventative IT support often experience less downtime, fewer unexpected expenses, and greater confidence that their technology is working for them—not against them.

Downtime Is More Expensive Than Most Businesses Realize

When technology stops working, business often comes to a standstill. Employees may be unable to access files, answer customer emails, process orders, or communicate with clients.

Even a short outage can quickly become expensive when multiple employees are unable to do their jobs.

The costs aren't limited to lost productivity. Missed deadlines, delayed customer service, interrupted sales, and damaged customer relationships can all have long-term effects.

Managed IT focuses on identifying potential issues before they grow into business disruptions. Continuous monitoring allows technicians to detect warning signs such as failing hardware, storage problems, or network issues before they cause an outage.

Preventing just one major interruption can often save far more than the cost of ongoing IT support.

Small Problems Become Big Problems

Technology rarely fails without warning. Hard drives begin reporting errors. Servers run low on storage. Software falls behind on updates. Backup jobs begin failing. Security alerts appear that go unnoticed.

Without someone actively monitoring these systems, small issues continue to grow until they become expensive emergencies. Routine maintenance allows these problems to be addressed while they are still minor, reducing both repair costs and business disruption.

Fixing a small issue today is almost always less expensive than recovering from a major failure tomorrow.

Security Is an Investment, Not an Expense

Cybersecurity has become one of the largest financial risks facing small businesses. A ransomware attack, phishing scam, or compromised email account can lead to days of downtime, lost revenue, legal expenses, regulatory penalties, and damage to customer trust.

Managed IT providers continuously monitor systems for suspicious activity, install security updates, verify backups, review user accounts, and help

employees recognize common cyber threats.

These preventative measures dramatically reduce the likelihood of costly security incidents. Rather than paying for recovery after an attack, businesses invest in reducing the chances of an attack succeeding in the first place.

Predictable Costs Make Budgeting Easier

Unexpected technology failures often come with unexpected invoices. Emergency service calls, replacement hardware, data recovery, and after-hours support can quickly exceed what many businesses planned to spend on IT.

Managed IT replaces unpredictable repair costs with consistent monthly budgeting. Business owners know what to expect each month while receiving ongoing monitoring, maintenance, security management, software updates, and technical support.

This allows organizations to plan future technology investments instead of constantly reacting to unexpected failures.

Employees Stay Productive

Employees lose valuable time every time they experience slow computers, unreliable Wi-Fi, software errors, or recurring technical problems.

While each issue may only take a few minutes to resolve, those minutes add up across an entire organization.

Proactive maintenance keeps systems running efficiently through regular updates, performance optimization, hardware monitoring, and preventative maintenance.

When employees spend less time waiting on technology, they spend

more time serving customers and growing the business.

Improving productivity is one of the most overlooked financial benefits of managed IT services.

Planning Instead of Reacting

Technology should support your long-term business goals. Managed IT providers don't simply respond to support tickets—they help businesses plan for future growth.

Regular technology reviews help identify aging equipment, warranty expirations, software licensing needs, cybersecurity improvements, and infrastructure upgrades before they become urgent.

This strategic planning helps businesses spread technology investments over time instead of facing large, unexpected replacement costs.

Better planning also reduces the risk of purchasing unnecessary equipment or replacing systems before it's truly needed.

Technology Should Help Small Businesses Grow

Reliable technology gives employees the confidence to work efficiently while allowing business owners to focus on running their company instead of worrying about technical problems.

When systems are monitored, maintained, and secured every day, businesses experience fewer disruptions, stronger cybersecurity, and greater operational efficiency.

Managed IT isn't simply about fixing what's broken—it's about keeping your business productive, protected, and prepared for the future.

As technology continues to play a larger role in every organization, having a trusted IT partner becomes one of the smartest investments a business can make.



THIS MONTH'S PRODUCT
SPOTLIGHT

CLICK TO VIEW A SHORT
VIDEO!



GRAYMAIL PROTECTION
FILTER

CLEAR YOUR
INBOX



NEVER MISS
IMPORTANT EMAILS

ALL GRAYMAIL PUT
INTO ONE PLACE



REDUCE EMAIL
NOTIFICATIONS

SUMMER HEAT CAN SHORTEN THE LIFE OF YOUR
LAPTOP

As temperatures rise during the summer months, most people think about protecting themselves from the heat—but your laptop can suffer from it too.

Whether you're working from a patio, leaving your computer in a hot vehicle, or simply using it in a warm office, excessive heat can have a significant impact on both performance and lifespan.

Laptops rely on proper airflow to keep internal components cool. When vents become blocked or the surrounding temperature is too high, the system has a much harder time removing heat. To protect itself, the laptop may automatically slow down its processor, causing applications to run more slowly and reducing overall performance.

Prolonged exposure to heat can also shorten the lifespan of critical components. Batteries are especially sensitive to high temperatures, and repeated overheating can reduce their ability to hold a charge over time.

Heat can also place additional stress on storage drives, memory, and other internal hardware, increasing the likelihood of unexpected failures.

Fortunately, a few simple habits can help keep your laptop running safely. Always use your laptop on a hard, flat surface so the cooling vents remain unobstructed.

Avoid leaving it inside a parked vehicle, where temperatures can quickly exceed 120°F, and keep it out of direct sunlight whenever possible. Regularly cleaning dust from cooling vents also helps maintain proper airflow.

If your laptop frequently feels unusually hot, the cooling fan runs constantly, or the system unexpectedly shuts down, it may be time for a professional cleaning or hardware inspection.

At Ferguson Computer Services, we can inspect your laptop, clean its cooling system, and ensure it's operating at safe temperatures so you can stay productive all summer long.

WHY REBOOTING YOUR COMPUTER IS IMPORTANT

Many people leave their computers running for days or even weeks without restarting them. While it may seem harmless, regularly rebooting your computer is one of the simplest ways to improve performance, reliability, and security.

Over time, programs consume memory, temporary files accumulate, and background processes continue running even after applications are closed. This can cause your computer to become slower, less responsive, or more prone to unexpected errors.

A simple restart clears temporary data, refreshes system resources, and allows your operating system to start with a clean slate.

Rebooting is also an important part of cybersecurity.

Many Windows updates, security patches, and software fixes are not fully installed until the computer is restarted. Delaying a reboot can leave your system waiting to apply critical updates that help protect against newly discovered vulnerabilities.

For most business users, restarting your computer at least once a week is a good habit. If you receive a notification that updates are ready to install, don't ignore it—a quick reboot now can prevent bigger problems later.

At Ferguson Computer Services, we can help keep your computers running at their best through proactive maintenance, performance optimization, and routine health checks.

HOW TO SAFELY OPEN A DOCUSIGN EMAIL WITHOUT FALLING
FOR A SCAM

Electronic signatures have become an essential part of doing business. Whether you're signing contracts, approving invoices, completing HR paperwork, or reviewing customer agreements, platforms like DocuSign allow documents to be securely signed in just a few clicks. Because of its popularity and widespread use, DocuSign has also become one of the most frequently impersonated services used by cybercriminals.

Attackers know that employees are accustomed to receiving document requests throughout the workday. If they can make a fake DocuSign email look convincing enough, there's a good chance someone will click the link without thinking twice. Their goal is often to steal login credentials, install malware, or gain access to sensitive business information.

Fortunately, there are several simple ways to identify suspicious DocuSign emails before they become a security incident.

Start by Asking One Question

Before opening any document request, ask yourself, "Was I expecting this?"

If you know the sender and have been waiting for a contract or document, that's a good sign. However, if the email arrives unexpectedly or references a document you've never heard of, take a moment to investigate before clicking anything.

Cybercriminals often rely on curiosity or urgency to convince people to act quickly. An unexpected invoice, purchase agreement, or payroll document may seem important enough to open immediately, but slowing down for a few seconds can prevent a costly mistake.

Verify the Sender

One of the easiest ways to spot a phishing email is by checking the sender's email address.

Don't rely solely on the display name, as attackers can easily make an email appear to come from "DocuSign" or even someone within your own company. Instead, view the full email address and confirm it matches the organization that supposedly sent the document.

Misspelled company names, extra characters, or unfamiliar domains are all warning signs that the email may not be legitimate.

Watch Out for Urgency

Messages that claim your document will expire within minutes, threaten account suspension, or insist on immediate action are designed to pressure recipients into clicking without thinking.

While legitimate businesses sometimes include deadlines, they rarely use aggressive language to force an immediate response. If an email makes you feel rushed, it's worth taking a closer look before proceeding.

Hover Before You Click

Before selecting the Review Document button, hover your mouse over the link without clicking it.

Most email programs will display the destination website. If the link points somewhere unrelated to DocuSign or redirects to an unfamiliar website, do not open it.

While not every malicious link is obvious, checking where a button leads is one of the easiest habits you can develop to avoid phishing attacks.

Be Careful with Attachments

It's important to understand how DocuSign normally delivers documents. Legitimate DocuSign requests are generally viewed through a secure web browser. They typically do not require you to download ZIP files, executable programs, or Microsoft Office documents that ask you to enable macros before viewing the document.

Unexpected attachments should always be treated with caution. Files ending in .zip, .exe, .js, .scr, or macro-enabled Office documents are commonly used to distribute malware.

If you're asked to install software just to view a document, stop immediately and verify the request before continuing.

Verify Through Another Method

If something doesn't seem right, don't rely on the email itself to confirm its authenticity.

Instead, contact the sender using a phone number or email address you already know is legitimate. A quick phone call can confirm whether the document request is genuine and may prevent a phishing attack from affecting your entire organization.

When in Doubt, Ask

Cybercriminals continue to improve their phishing techniques, making fraudulent emails more convincing every year. Even experienced users occasionally receive messages that are difficult to identify.

If you are ever unsure whether a DocuSign request is legitimate, don't take the risk. It's always better to ask for verification than to deal with the consequences of a compromised account or malware infection.





WHAT MICROSOFT'S NEW WINDOWS 11 UPDATE MEANS FOR SMALL BUSINESS

Microsoft is continuing to improve Windows 11 with its upcoming version 26H2 update, focusing on making everyday tasks easier while giving users more control over how Windows looks and works.

Instead of introducing dramatic changes, Microsoft has concentrated on improving the features people use every day, including the Start menu, Taskbar, and Windows Search. These updates are expected to begin rolling out later this year through Windows Update.

While many software updates happen quietly in the background, this release includes several changes that business users will notice immediately.

A More Flexible Start Menu

One of the biggest improvements is a redesigned Start menu. Users will have more control over its layout, allowing them to resize it and organize sections more effectively.

For businesses, this means employees can customize their workspace without unnecessary distractions, making frequently used applications easier to find.

Better Windows Search

Searching for files has long been a frustration for many Windows users. Microsoft is improving Windows Search by prioritizing local files and recently used documents instead of displaying unnecessary web results.

The updated search experience is also better at finding files even when names are misspelled or only partially remembered. Businesses that store large numbers of documents on employee computers should notice faster and more accurate search results.

More Control Over the Taskbar

Another welcome improvement is additional Taskbar customization. Users will once again be able to position the Taskbar in different locations and even reduce its size to create more usable screen space. These changes give employees greater flexibility to organize their desktops in a way that best supports their workflow.

While these may seem like small adjustments, even minor improvements to the tools employees use every day can have a positive impact on productivity.

Improved Update Experience

Microsoft is also working to make Windows updates less disruptive. Recent improvements reduce unnecessary restarts while continuing to deliver important security updates and feature enhancements.

The company is also introducing changes behind the scenes that help simplify future updates and improve the overall reliability of Windows.

Keeping computers updated remains one of the easiest ways to protect against newly discovered security vulnerabilities.

Why Businesses Should Prepare

Although these updates are designed to improve the Windows experience, every major feature release should still be tested before being deployed across an entire organization.

Businesses often rely on specialized software, printers, scanners, accounting applications, and other hardware that should be verified for compatibility before widespread installation.

Let us help. Here at Ferguson Computer Services we are always dedicated to ensuring that you are not only running smoothly but also taking advantage of all the features Windows 11 has to offer.

Microsoft continues to evolve Windows with new features, improved security, and better productivity tools.

Keeping your systems current helps ensure your business remains secure while giving employees access to the latest capabilities.

At Ferguson Computer Services, we help businesses manage Windows updates, verify software compatibility, and ensure new Microsoft features are deployed safely with minimal disruption.

By taking a proactive approach to updates, your organization can enjoy the latest improvements while reducing downtime and avoiding unexpected compatibility issues.



WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we'll gift them their first month of service at no charge AND we'll gift you a \$500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I'll take it from there. I personally promise we'll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan



We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly and would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.



[Leave a Google Review](#)

[Leave a Facebook Review](#)

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a \$50 gift card to Amazon.

Here is August's question of the month:

How do Small Problems become Big Problems in Technology?

